SYSTEM FOR PROTECTING DOMAIN SYSTEM CONFIGURATIONS FROM USERS WITH LOCAL PRIVILEGE RIGHTS

Abstract

A group change lockout system for protecting the configuration of a securable object in an operating system from members of a locally privileged group, such as the local administrators group, when a security descriptor exists for the securable object that includes a discretionary access control list (DACL). A copy of the security descriptor is made. Then a new access control entry (ACE) is added to the DACL in the copy. This new ACE specifies denying the local administrators group an access right to the securable object. Then the security descriptor in the operating system is overwritten with the copy.